SECRET

16 June 1980

25X1A MEMORANDUM FOR: [redacted]
Chief, Management Staff
Office of Data Processing

25X1A FROM: [redacted]
Deputy Director for Applications
Office of Data Processing

SUBJECT: Draft Security Requirements for Automated Information Systems Located in Overseas Installations (U)

1. Applications personnel have reviewed the draft requirements submitted by the Information Systems Security Group, Office of Security. Since we recognize the importance of writing policy in this area we recommend that the following comments be incorporated in the next revision. (U)

2. The purpose of automating field stations is to make them more efficient and to reduce the vulnerability of information, especially if a station is overrun. Although the draft specifies that removable data storage media shall be used (IV.D.1.c), the draft does not address how data should be stored on the media. Considering the possibility of large information banks in the field, stronger guidelines are needed as to what and how much data should be kept in the field and under what conditions. (S)

For instance, should the data stored on field media be encrypted? (S)

If a cassette or a floppy disk were compromised, the problem of damage assessment is not addressed. Since there is no requirement for maintaining volume data set catalogs, the Agency would not know what data was lost. (S)

3. The requirement in IV.D.2.4 for system software to handle all interrupts in a known and secure manner implies that only provably secure operating systems would be allowed. Such operating systems are being developed but are not available now. The draft does not address system software certification or waiver procedures. (U)

SECRET

4. In paragraph IV.D.5.a.2 the draft specifies the ''only those terminals designated for the security classification access level being processed shall be logically connected...''. The draft could easily specify that terminals not so designated be electrically disconnected by means of a patch panel or other similar arrangement. The specification of ''logically'' implies that the system software would control access and this is an unneccessary spillage risk. (S)

5. The requirement for each data file to be controlled by a file password and indicators to describe to the system the type of access authorized (IV.D.5.b.1) is unrealistic for the class of machine planned for the field. Since each dataset must reside on removable media and each storage disk, tape, etc., is to be marked, why not specify that only those media marked at the appropriate level be installed on the system? (S)

6. In the following paragraph (IV.D.5.b.2), access to the master data file is limited to the ADP System Security Officer. This is short sighted and not practical. First, there should always be a backup for this function. And, second, there is a need in some installations for backup of datasets that requires automatic linkage to the master data file. The password file should be protected by encryption such that a system dump or system spillage will not compromise this file. (S)

7. It is puzzling why the password procedures (IV.D.5.c) do not apply to stand-alone word processing terminals since this class of terminals can read and write the same data sets as other ADP systems, and up to the same classification levels. (U)

8. The section on Data Processing (V.B.) regarding abnormal data processing system operation is not practical. A runaway tape or a disk head crash should not cause the system to be stopped. This section should be rewritten to be more specific and should concentrate on events that have security implications. For instance, a reported spillage to a terminal or printer should be investigated and would be a valid reason to stop the system. (S)

9. The section on System Maintenance/Modification may not recognize that the Agency does and will probably continue to use contractor personnel for on-site maintenance and field modification of equipment. (U)

10. The certification of the ISSO on system software modifications in section VII.B.b requires technically expert people to be meaningful. Since these experts are in short supply, even in ADP components, this requirement could be a bottleneck in software updates. (U)

11. The key to emergency procedures, as mentioned before, is in limiting the amount of data stored in the field, not in trying to sanitize or destroy it during an emergency. The draft does not specify that the procedures be exercised so that they are proven and field personnel are fully familiar with them. A possible oversight is that there is no requirement that the ADP Systems Security Officer be responsible for having ADP personnel read the procedures. (U)

12. Equipment procurement sterility is not addressed in the draft. Will there be any policy or guidelines regarding equipment that is Agency unique? (S)

25X1A

[redacted]